REMARKS/ARGUMENTS

Reconsideration and allowance of this application are respectfully requested. Currently, claims 4-8, 23-25, 29-38 and 40-46 are pending in this application.

Rejections Under 35 U.S.C. §103:

Claims 3, 7, 23-25, 27, 31 and 33-43 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Bachman et al (U.S. '621, hereinafter "Bachman") in view of Carlson et al (U.S. '046, hereinafter "Carlson"). Applicant respectfully traverses this rejection.

In order to establish a *prima facie* case of obviousness, all of the claim limitations must be taught or suggested by the prior art. The combination of Bachman and Carlson fails to teach or suggest all of the claim limitations. For example, the combination fails to teach or suggest the following limitations required by independent claim 23 and its dependents:

> "i) if no address token which uniquely identifies the user is contained in the client-side persistent information accompanying said request:
>
> > generating an address token which uniquely identifies the terminal address of the user, the generated address token replacing an IP address of the client terminal as a way of subsequently re-identifying the terminal address of the user;
> >
> > transmitting the generated address token to the client application in a client-side persistent information packet so that the address token can be used to uniquely re-identify the user when re-transmitted with user authentication data to the resource server; and
> >
> > storing said address token for the user; and
>
> ii) if an address token is received which accompanies user authentication data, using said address token to uniquely re-identify the address of the terminal from which the original document request was received;"

The combination also fails to teach or suggest the following limitations required by independent claim 25 and its dependents:

> "sending the user an unvalidated tag to enable subsequent re-identification of the terminal address of the user;
> authenticating the user by performing:
> receiving user authentication data with a returned unvalidated tag at the resource server for the user from the client terminal having no unique IP address,
> validating said authentication data by determining if said authentication data corresponds to equivalent stored authentication details, and if so:
> updating the tag to a validated user identifying tag;
> transmitting the validated user identifying tag to said client terminal for storage thereon, the validated user identifying tag being arranged to enable the client terminal to retransmit the validated user identifying tag with document requests directed at said resource server; and"

The above-identified limitations relate to sending the user an unvalidated address token or tag to re-identify the terminal address of a user. In particular, an unvalidated address token or tag is sent to a user to re-identify the terminal address of a client terminal having a non-unique IP address. The unvalidated address token or tag is sent **prior** to any user identity information being provided. The unvalidated address token or tag is then returned along with user authentication data. The user authentication data sent with the unvalidated address token or tag is used to validate (or not validate) the already existing address token or tag.

The present invention thus addresses a situation where the IP address of a client terminal is not uniquely known, and the authenticating server must have some way of identifying the terminal address of a user. This identification is accomplished by sending the user an unvalidated address token or tag prior to any user identity information (e.g., user name and password data) being provided by the user. User authentication data is provided with the unvalidated address token or tag upon its return for authentication purposes.

In the present invention, the user may attempt to "log-in" with authentication data by returning a previously provided address token or tag which re-identifies the non-unique IP address of the client terminal. In contrast, Bachman explicitly discloses a user attempting to "log-in" with authentication data prior to even generating a token. Bachman fails to disclose anything even relating to sending an unvalidated address token or tag to re-identify a client terminal from its non-unique IP address.

The Advisory Action apparently alleges that col. 6, lines 20-37 and 43-50 discloses the above-noted limitations. Applicant respectfully disagrees. Bachman clearly discloses in col. 2, lines 13-15 that "The token is **<u>created</u> by combining user identity information with random information and table address information** in a way that has a high attack work factor so that it can effectively not be duplicated (emphasis added)." Bachman thus explicitly discloses that the user identity information is used to create the token. While Bachman requires a user to provide authentication data (e.g., user name and password for log-in purposes) prior to generating a token, the present invention requires a user to provide authentication data with a token that has been previously provided.

Col. 6, lines 20-37 and 43-50 (specifically identified in the Advisory Action) of Bachman discloses comparing stored token information with received token information to determine if a request is to be honored based upon the stored and received token information indicating that the received token is a valid unexpired token. In particular col. 6, lines 43-49 of Bachman states "If the token is found to be invalid, or in the alternate embodiment of block 431, if the token was received from an IP address other than stored in the session table, the request is not processed by a login menu is sent to the user at block 403 so as to determine if the user is an authorized user as was previously described with respect to these blocks 403 and 405." Blocks 403 and 405 teach generating a token based on the user identification information (as described above). Indeed, col. 5, lines 23-37 of Bachman states the following:

> "The user enters identity information such as a user ID and a memorized password that can be used to verify that the person who remembered the password is an authorized user. The user then submits the login page at block 405. At block 406, the host 19 has verified correspondence between the ID and password and at block 407, the session object 217 generates a token as described earlier with respect to FIG. 2.
>
> The token can be represented by the expression:
>
> $E_k(f(ID),R,I)$
>
> where E subscript k is the encryption using the encryption key k of the argument value in the parentheses. f(ID) is a function such as a hash function of the users identity information. R is a random number and I is the index to an entry in the session table 221."

Accordingly, it is quite clear from Bachman that the user identity information is used to initially generate the token. Fig. 2 of Bachman clearly shows the following sequence of events for a customer login in from a user at a client 23 to a host 19:

i) The server program requests via web requestor object 211 and customer object 213 login ID and password information from the host object 215. (See Col. 3, lines 25 to 26).

ii) The host object 215 passes the user identification and password to the host 19 - if there is a match, then the user is an authorized user and the host 19 returns data which enables an HTML page object 219 to format a menu page or form to be sent to the authorized user.

iii) The user identity information is passed to the session object 217 which sets up a session by generating a session token from a hash of the identity information, from an index and from random numbers R0 and R1.

iv) The identity information, random information R0,R1, and other information such as an account list and the page transmission time T are stored in a session table 221 at the index entry I used to generate the token.

Rather than use received authentication data to validate an already-existing address token or tag also received by a server as respectively required by independent claims 23 and 25, Bachman therefore discloses using user identity information to initially generate a session token. Accordingly, Bachman fails to disclose receiving, at the server, an unvalidated address token or tag and then validating this address token or identifying tag based on received authentication data. The address token or tag is received and already exists at the time the authentication data is processed at the server to perform validation. Bachman discloses using the user identity information to initially generate a token. After the unvalidated address token or tag is validated by the received authentication data, the validated address token or identifying tag is then transmitted back to the client terminal.

In the present invention, a resource server sends the user an unvalidated address token or tag (e.g., a unique large number). The user then enters his authentication data (e.g., user name and password), and this authentication data is provided along with the return of the unvalidated address token or tag for authentication. The unvalidated address token or tag enables the application server to identify the user for whom the password and user identity information process is to be formed as no other unique address information is available.

Bachman suggests that the host must know the name of the user in order to return a token. For example, col. 3, lines 30-34 of Bachman states "If the password and identity information correspond, the user is an authorized user and the host 19 also returns an account list and other practical information that can be used by the HTML page object

219 to format a menu page or form to be sent to the authorized user." Bachman therefore does not contemplate how to identify a user for authentication purposes if the user's terminal IP address is not specifically known (i.e., the client terminal has no unique IP address) since Bachman suggests that it is known for the token to be returned to client. Bachman's embodiment thus requires knowledge of the address.

Accordingly, Applicant respectfully submits that the rejection under 35 U.S.C. §103 in view of Bachman and Carlson be withdrawn.

Claims 4 and 28 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Bachman, Carlson and Johnson et al (hereinafter "Johnson"). Claims 2 and 26 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over the <u>three</u>-way combination of Bachman, Carlson and Kirsch. Claims 5, 6, 29 and 30 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over the <u>four</u>-way combination of Bachman, Carlson, Johnson and See et al. None of these third or fourth references (Johnson, Kirsch and/or See) remedy the above-described deficiencies of the Bachman/Carlson combination. Applicant thus respectfully requests that the above-noted rejections under 35 U.S.C. §103 be withdrawn. Applicant notes that claims 2, 26 and 28 have been canceled.

<u>New Claims</u>:

New claims 44-46 have been added to provide additional protection for the invention. New claim 44 requires, *inter alia*, "checking if the request contains a validated or unvalidated token enabling the terminal of the user to be subsequently re-identified, and if not, providing an address token to the user in an initial cookie containing in a field an identifying tag which replaces the non-unique IP address of the terminal as a means for subsequently re-identifying the terminal." Applicant thus submits that claim 44 and its dependents are allowable.

<u>Conclusion</u>:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: ____________________
Raymond Y. Mah
Reg. No. 41,426

RYM:sl
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4044
Facsimile: (703) 816-4100